# TTP Detail – T1559.002

## TTP Information

Name: Dynamic Data Exchange

Description: Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands. DDE is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by [Component Object Model](https://attack.mitre.org/techniques/T1559/001), DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys.(Citation: BleepingComputer DDE Disabled in Word Dec 2017)(Citation: Microsoft ADV170021 Dec 2017)(Citation: Microsoft DDE Advisory Nov 2017)

Microsoft Office documents can be poisoned with DDE commands, directly or through embedded files, and used to deliver execution via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros.(Citation: SensePost PS DDE May 2016)(Citation: Kettle CSV DDE Aug 2014)(Citation: Enigma Reviving DDE Jan 2018)(Citation: SensePost MacroLess DDE Oct 2017) Similarly, adversaries may infect payloads to execute applications and/or commands on a victim device by way of embedding DDE formulas within a CSV file intended to be opened through a Windows spreadsheet program.(Citation: OWASP CSV Injection)(Citation: CSV Excel Macro Injection )

DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). DDE execution can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* GravityRAT
* HAWKBALL
* KeyBoy
* POWERSTATS
* PoetRAT
* RTM
* Ramsay
* Valak

## APTs (Intrusion Sets)

* APT28
* APT37
* BITTER
* Cobalt Group
* FIN7
* Gallmaker
* Leviathan
* MuddyWater
* Patchwork
* Sidewinder
* TA505